

**Department of Homeland Security  
Information Analysis and Infrastructure  
Protection  
Daily Open Source Infrastructure Report  
for 01 May 2003**

Current Nationwide  
Threat Level is



[For info click here](http://www.whitehouse.gov/homeland)  
[www.whitehouse.gov/homeland](http://www.whitehouse.gov/homeland)

**Daily Overview**

- Reuters reports about 100 postal workers and customers were evacuated from a post office in Gilbert, AZ after a yellow powdery substance was discovered leaking from a package. (See item [10](#))
- Microsoft has released Microsoft Security Bulletin MS03-016: Cumulative Patch for BizTalk Server. (See item [21](#))
- eWEEK reports a new vulnerability in Oracle Corporation's database software puts not only the information in the database at risk, but in some cases, also can lead to a compromise of the operating system. (See item [23](#))

**DHS/IAIP Update *Fast Jump***

**Production Industries:** [Energy](#); [Chemical](#); [Defense Industrial Base](#)

**Service Industries:** [Banking and Finance](#); [Transportation](#); [Postal and Shipping](#)

**Sustenance and Health:** [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

**Federal and State:** [Government](#); [Emergency Services](#)

**IT and Cyber:** [Information and Telecommunications](#); [Internet Alert Dashboard](#)

**Other:** [General](#); [DHS/IAIP Web Information](#)

**Energy Sector**

**Current Electricity Sector Threat Alert Levels:** **Physical:** Elevated, **Cyber:** Elevated

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

1. **May 30**, — Massachusetts oil spill's repercussions feared. Environmental officials were still assessing the impact of Sunday's spill at Buzzards Bay, off the southeastern Massachusetts coast. and they were optimistic that the weather would start making the cleanup job easier. Officials said it was particularly unfortunate that the spill happened just as many birds – including endangered roseate terns – are nesting and fish are gathering for spawning runs. A number of seabirds were contaminated by oil and there was concern about marine life. The spill also is hurting commercial shellfishermen who harvest softshell clams, scallops and oysters from the bay. State officials shut down shellfishing Monday in all the bay except the northernmost portion leading into the Cape Cod Canal. **On Wednesday morning**,

the damaged barge was being towed to a fuel terminal in Sandwich, Coast Guard Petty Officer Andrew Shinn said. The fuel was drained Tuesday from the damaged compartment, and the rest of the oil will be unloaded at the terminal, Shinn said. The Coast Guard is still investigating why the barge, owned by Bouchard Transportation Co., entered shallower waters. The results of drug and alcohol tests performed on the crew were not immediately available.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A59056-2003Apr 30.html>

2. *May 30, New York Times* — **Problems are compounded at Indian Point plants. A day after a power failure at the Indian Point nuclear plant complex, officials were dealing with new problems: an early-morning fire, and criticism of the long hours that security officers there are forced to work.** The criticism was prompted by a letter to security officers dated April 21 from an official of the Entergy Corporation, which owns the plants. The letter alerted the officers to the likelihood of working "five 12-hour days and occasionally six 12-hour days" to prepare for an antiterrorism drill in early summer. **Today the Nuclear Regulatory Commission (NRC) sent out new orders to the nation's nuclear plants concerning security preparations.** Neil A. Sheehan, a spokesman for the commission, said that the agency sent out three orders, including one that limits security officers to working "no more than 48 hours per week during normal operating times." The fire and power failure occurred within hours of each other and led to the shutdown of both reactors, but were not related to the issue of security, Sheehan said. **Plant officials say that some insulating material ignited on the outer casing that houses the turbine. Lubricating oil had apparently leaked onto the insulation and that may have caused the fire, but how the oil got there is still under investigation,** said Jim Steets, an Entergy spokesman.

Source: <http://www.nytimes.com/2003/04/30/nyregion/30NUKE.html>

3. *May 29, Reuters* — **U.S. beefs up atomic power plant security rules. The U.S. Nuclear Regulatory Commission (NRC) on Tuesday ordered atomic power plant operators to further tighten security at the nation's 103 nuclear reactors to better thwart attacks or sabotage.** The changes are part of the NRC's effort to beef up security at nuclear reactors in the wake of the September 11, 2001, attacks on New York City and the Pentagon. The NRC said it had approved three security orders, including changes in the so-called design basis threat that private security forces protecting the power plants must be prepared to meet. **Details of the changes will not be made public, the NRC said. The other two orders specify work schedules, training and qualifications required of plant security guards who are hired by utilities to protect their facilities.** The orders are effective immediately, the NRC said. Some U.S. lawmakers and activist groups are concerned that a September 11-type attack against a nuclear plant could penetrate the reactor or pool where used fuel is stored and spread deadly radioactive materials for miles.

Source: [http://www.energycentral.com/sections/news/nw\\_article.cfm?id=3807337](http://www.energycentral.com/sections/news/nw_article.cfm?id=3807337)

4. *May 29, Reuters* — **U.S. Senate panel to finish energy bill this week. Senate lawmakers plan to finish writing legislation this week aimed at carrying out the biggest overhaul of American energy policy in a decade, hoping to reach an agreement with the House of Representatives that has passed a much different energy bill.** The energy legislation is expected to be considered by the full Senate in May, but differences with the House bill would have to be hammered out before President George W. Bush could sign a bill into law. **The**

**Senate Energy Committee will debate on Tuesday the transportation fuels provision of its bill;** panel members are expected to consider a proposal to double the production of ethanol-blended gasoline over the next decade. **The Senate committee will also vote Tuesday on provisions in the legislation that promote energy production on Indian lands and general energy research and development. On Wednesday, the committee tackles language to improve the U.S. electricity grid.** Another major difference in the approaches of the two bodies is that **the House bill allows oil drilling in Alaska's Arctic National Wildlife Refuge, while the Senate legislation denies energy firms access to the refuge.**

Source: [http://www.energycentral.com/sections/news/nw\\_article.cfm?id=3806480](http://www.energycentral.com/sections/news/nw_article.cfm?id=3806480)

[\[Return to top\]](#)

## **Chemical Sector**

Nothing to report.

[\[Return to top\]](#)

## **Defense Industrial Base Sector**

5. *April 29, The Center for Strategic and Budgetary Assessments* — **Shaping the future of Northern Command.** The United States Northern Command (NORTHCOM) is a new military headquarters charged with defending the American homeland. The command was established on October 1, 2002 in response to the terrorist attacks on Washington DC and New York City, Enhancing the role and missions of NORTHCOM could do much to further improve U.S. domestic security over the long term. **Despite the creation of the new headquarters, other commands have significant roles related to domestic security. More robust and formal means are needed to integrate their activities with NORTHCOM.** NORTHCOM also needs a more robust organization and additional resources, including a sub-regional command structure, a more visible presence in Washington, assigned forces designed to perform homeland security tasks, and an expanded training mission. The command could also serve as a catalyst for transformation. **Many of the requirements for homeland defense, such as expanded situational awareness and efficient, networked systems that can immediately and accurately direct forces to perform critical missions, parallel those mentioned as desirable for U.S. general purpose forces.**

Source: <http://www.csbaonline.org/4Publications/Archive/B.20030429.NORTHCOM/B.20030429.NORTHCOM.pdf>

[\[Return to top\]](#)

## **Banking and Finance Sector**

6. *April 30, U.S. Department of the Treasury* — **Treasury issues proposed anti-money laundering rules for the Securities and Commodities industry.** The Department of the Treasury and the Financial Crimes Enforcement Network on Wednesday issued three separate proposed rules under the USA Patriot Act that would expand anti-money laundering regulation to commodity trading advisors and securities investment advisers,

as well as require suspicious activity reporting by futures commission merchants. The proposed rules would amend the Bank Secrecy Act (BSA) regulations as part of Treasury's continuing implementation of the USA PATRIOT Act. Interested parties will have sixty days to comment on the proposed rules following their publication in the Federal Register, which is expected to occur later this week. These rules will serve as additional tools in the Administration's continuing effort to fight illicit money laundering.

Source: <http://www.treasury.gov/press/releases/js333.htm>

7. *April 30, New York Times* — **Global Crossing sale under scrutiny.** The federal government has opened a formal investigation into the proposed buyout of Global Crossing by companies in Hong Kong and Singapore, people briefed on the inquiry said yesterday. **The investigation was started on Monday by the Committee on Foreign Investment in the United States, which is managed by the Treasury Department and which had been studying the proposed foreign investment into Global Crossing, the people said.** Becky Yeaman, a spokeswoman for Global Crossing, a bankrupt owner of communications networks, said, "The process is confidential and we don't comment on it." **Hutchison Whampoa in Hong Kong and Singapore Technologies Telemedia have proposed to buy controlling shares of Global Crossing. But departments in the federal government, as well as members of Congress, have remained wary of the deal because it would pour considerable amounts of foreign-based money into a company based in Madison, NJ. Also, Global Crossing's worldwide network is used by the United States government.**

Source: <http://www.nytimes.com/2003/04/30/business/worldbusiness/30GLOB.html>

[[Return to top](#)]

## **Transportation Sector**

8. *May 29, New York Times* — **States would decide service under Bush's Amtrak plan.** The Bush administration proposed a national rail plan, on Tuesday, to restructure Amtrak and leave important decisions about train service, including long-distance routes, to the states. "We do not propose to eliminate Amtrak, but we do propose comprehensive structural changes," Michael Jackson, the deputy transportation secretary, said at a Senate Commerce Committee hearing. **The current five-year Amtrak authorization as a federal corporation to provide the national passenger rail service expires in September, and Congress is weighing proposals to overhaul the railroad and chart a new course for a national rail system.** Jackson's outline closely follows principles advanced last year by Transportation Secretary Norman Y. Mineta to dismantle Amtrak's reliance on federal subsidies to survive. **Amtrak will receive a \$1.05 billion subsidy this year after losing more than \$1 billion in 2002.** "It would be irresponsible to eliminate Amtrak altogether, but it would be an equal folly not to reform a corporation suffering such a persistent and thoroughgoing crisis," Jackson said.

Source: <http://www.nytimes.com/2003/04/30/politics/30AMTR.html>

9. *May 29, KSL TV* — **Remote-controlled trains cause community concerns.** An issue of safety is starting small but promises to grow in Utah. **It centers on a new trend in the Railroad industry not many people know about: locomotives run by remote-control.** Union Pacific (U-P) confirms—it's training employees to run this diesel engine here—part of a new industry standard that that uses remote control technology. U-P says it's used mostly in

railyards In Canada, it's been used for a decade or so. But engineers across the nation are speaking out against remote control trains. **There have been serious remote control train accidents that have happened across the nation. One involved 25–thousand gallons of a hazardous chemical. Most involved property damage and a few serious injuries. In all, at least 40 have been documented since December of 2000.** Union Pacific says most of the accidents weren't caused by the technology—but were attributable to human error and would have happened anyway. The company says remote technology has advanced so safety isn't an issue. But engineers say safety—even close to railyards—is in question. **In fact 15 other communities have passed resolutions banning remote control trains from their city limits. But the resolutions are not legally binding, so in atleast some case, the trains are running anyway.**

Source: <http://tv.ksl.com/index.php?nid=39ont>>

[\[Return to top\]](#)

## **Postal and Shipping Sector**

10. *April 29, Reuters* — **Arizona post office evacuated over yellow powder. About 100 postal workers and customers were evacuated from a post office in Gilbert, AZ on Tuesday after a yellow powdery substance was discovered leaking from a package, authorities said.** Three postal workers were decontaminated at the scene and sent to hospitals. One 40–year–old woman complained of a headache and eye irritation, a 56–year–old woman suffered from a headache, and a 33–year–old man had difficulty breathing, fire officials said. The facility was cleared at about 9 a.m. PDT when workers unloading packages on the loading dock noticed the substance and alerted supervisors, officials said. **A hazardous materials team tested the substance to rule out the presence of ricin or anthrax, said Gilbert Fire Captain Robert Foster.**

Source: <http://www.reuters.com/newsArticle.jhtml?type=topNewsD=2653137>

[\[Return to top\]](#)

## **Agriculture Sector**

11. *April 30, Associated Press* — **Agriculture board approves chronic wasting disease rules. The Colorado Agriculture Board reluctantly has agreed to new rules that will set up a shared responsibility with the Division of Wildlife to crack down on the movement of elk infected with a deadly brain disease.** Chronic wasting disease (CWD) attacks the brains of infected animals, causing them to become emaciated, display abnormal behavior, lose bodily functions and die. There have been arguments about whether wild elk originally infected captive herds in Colorado or the captive herds passed along the infection. But because the problem affects both agencies, rules are being established for what animals can be imported into the state and how they can be transported between ranches in Colorado. **Under the plan those wanting to bring elk into the state first need to apply with the state veterinarian, who would decide whether the animals had been under surveillance for five years. He then would make a recommendation to the wildlife division.**

Source: [http://www.trib.com/AP/wire\\_detail.php?wire\\_num=107286](http://www.trib.com/AP/wire_detail.php?wire_num=107286)

12. *April 30, Age* — **Mystery surrounds \$26 billion wheat virus threat. Authorities today were searching for answers as to how a virus threatening Australia's \$26 billion grain industry had been found at a second site.** A nationwide emergency plan was activated last night to control the wheat streak mosaic virus. The virus, first detected at two CSIRO sites in Canberra, has now been found at a plant research centre in South Australia. **If further tests now being done confirm the two outbreaks are unrelated, it would mean the virus has managed to find ways of getting into Australia despite stringent quarantine conditions.**

Source: <http://www.theage.com.au/articles/2003/04/30/1051381984644.html>

[\[Return to top\]](#)

## **Food Sector**

Nothing to report.

[\[Return to top\]](#)

## **Water Sector**

Nothing to report.

[\[Return to top\]](#)

## **Public Health Sector**

13. *April 30, PhysicsWeb* — **Cold plasmas destroy bacteria. Researchers have devised a new method for killing bacteria using cold plasmas. The technique, developed by Mounir Laroussi at the Old Dominion University in Virginia and colleagues at the University of California in San Diego, could be used to sterilize medical equipment, food, and perhaps even decontaminate biological weapons.** The team exposed two types of bacteria those with and without outer cell membranes and studied the effect of the plasma with a scanning electron microscope. After an exposure of 10 minutes, both types of bacteria had been killed by ultraviolet radiation and free radicals from the plasma. In addition, the charged particles caused structural damage to outer cell membranes in only microseconds. The team believes that cold plasmas would also prove lethal to more dangerous bacteria and also viruses.

Source: <http://physicsweb.org/article/news/7/4/19>

14. *April 30, Associated Press* — **Possible drug targets found for anthrax. Scientists say they've found potential new targets for drugs and vaccines against the anthrax germ by deciphering and analyzing the bacterium's complete genetic makeup. Studying the 5.2 million "letters" of the germ's DNA code, researchers identified several genes that might play key roles in anthrax infections. Such genes might prove to be good leads for developing new treatments.** Anthrax infections respond to antibiotics if administered early enough, and a vaccine is already available. But scientists are always looking for clues to devising better medicines and vaccines by learning about the inner workings of a germ. The effort is especially crucial for anthrax, which can be lethal, because it is a potential weapon of future terrorism.

Source: [http://abcnews.go.com/wire/Living/ap20030430\\_1264.html](http://abcnews.go.com/wire/Living/ap20030430_1264.html)



15. *April 30, Reuters* — **Nearly 10,000 quarantined in SARS—panicked Beijing.** Nearly 10,000 people in the Chinese capital were under quarantine after the city confined residents of one building in the heart of the capital and another in a northern suburb, state media said. Beijing has been the hardest-hit area in the world, with nearly 1,350 reported cases of Severe Acute Respiratory Syndrome and 66 deaths. **Acting Mayor Wang Qishan said there had been panic in Beijing, which has seen frenzied buying of medicines and staple foods, and that the virus was threatening to overwhelm the health-care system.**

Source: <http://www.washingtonpost.com/wp-dyn/articles/A57610-2003Apr 30.html>

[\[Return to top\]](#)

## **Government Sector**

16. *April 30, General Accounting Office* — **GAO-03-322: Information Technology: terrorist watch lists should be consolidated to promote better integration and sharing.** Generally, the federal government's approach to using watch lists in performing its boarder security mission is decentralized and nonstandard, largely because these lists were developed in response to individual agencies' unique missions, including their respective legal, cultural, and systems environments. **Specifically, nine federal agencies – which prior to the creation of the Department of Homeland Security (DHS) spanned the Departments of Defense, Justice, State, Transportation, and Treasury – develop and maintain 12 watch lists.** These lists include overlapping but not identical sets of data, and different policies and procedures govern whether and how these data are shared with others. The extent to which such sharing is accomplished electronically is constrained by fundamental differences in the watch lists' systems architecture. **GAO recommends that the Secretary of DHS, in collaboration with the heads of the other departments and agencies that have and use watch lists, lead an effort to consolidate and standardize the federal government's watch list structures and policies.** DHS and other departments involved in this study generally agree with GAO's findings and recommendations.

Source: <http://www.gao.gov/new.items/d03322.pdf>

17. *April 30, New York Times* — **New devices to recognize bodily features on entry into the U.S.** Domestic-security agencies will begin this year to use computer equipment that recognizes fingerprints and other features to verify the identities of foreign visitors as they enter and depart the United States, Bush administration officials said on Tuesday. **They said the new security measures, which may also include the use of computerized facial-recognition machinery, are intended to block the entry of terrorists into the United States and to verify that foreign visitors leave on schedule.** Such biometric technology had been mandated by Congress for use beginning late next year in an entry and exit system for foreign visitors as a result of the attacks on Sept. 11, 2001. But in a speech on Tuesday, Homeland Security Secretary Tom Ridge said the department had decided to move up the time frame, with some of the body-recognition equipment in place by the end of this year. Department officials said that while the department had still not worked out many of the details of its biometrics program, it was likely that some computerized fingerprint and facial-recognition equipment would be installed at some international airports, border crossings and seaports within several months.

Source: <http://www.nytimes.com/2003/04/30/international/worldspecial/30HOME.html>

18. *April 29, Federal Computer Week* — **Ridge announces VISIT system.** Homeland Security Secretary Tom Ridge announced a new initiative on Tuesday to build an electronic check in/check out system that will keep track of noncitizens as they enter and leave the United States. **Ridge said the new program would replace the troubled Student and Exchange Visitor Information System and the National Security Entry–Exit Registration System (NSEERS), which requires citizens of certain countries to be fingerprinted and registered with the federal government. Both systems hit snags during development and came under fire from civil liberties groups. The new system, U.S. Visitor and Immigration Status Indication Technology system, or U.S. VISIT, will make it easier for legitimate tourists, students and business travelers to enter the United States using biometric identifiers. It is expected to be in place at air– and seaports by the end of this year, according to Ridge.** Ridge's newest initiative will eliminate the NSEERS program, which required citizens of countries such as Iran, Iraq, Libya, Sudan and Syria to register and be fingerprinted by the federal government. The student registration system will be folded into the new program to keep track of foreigners studying in the United States.

Source: <http://www.fcw.com/fcw/articles/2003/0428/web-ridge-04-29-03.asp>

19. *April 29, The White House* — **Administration Appointment: General John A. Gordon.** The President intends to appoint General John A. Gordon to be Assistant to the President and Homeland Security Advisor. General Gordon is currently Deputy Assistant to the President, National Director and Deputy National Security Advisor for Combating Terrorism. Previously, he served as Administrator of the National Nuclear Security Administration and Under Secretary for Nuclear Security at the Department of Energy. Prior to this, General Gordon served as Deputy Director of Central Intelligence. A retired four star general, General Gordon previously served as Special Assistant to the Air Force Chief of Staff for strategic planning.

Source: <http://www.whitehouse.gov/news/releases/2003/04/20030429-10.html>

[[Return to top](#)]

## **Emergency Services Sector**

20. *April 29, United State Fire Administration* — **2003 assistance to firefighters grant application preliminary data.** The Federal Emergency Management Agency (FEMA) and the United State Fire Administration (USFA) have received approximately 19,950 applications for the 2003 Assistance to Firefighters Grant program. **The total request of all departments, including the non–federal share, is around \$2.5 billion. For the 2003 program, Congress appropriated, and President Bush signed into law, \$750 million in direct assistance in support of the nation's firefighters and the services they deliver.**

Source: <http://www.usfa.fema.gov/inside-usfa/media/03-042903.cfm>

[[Return to top](#)]

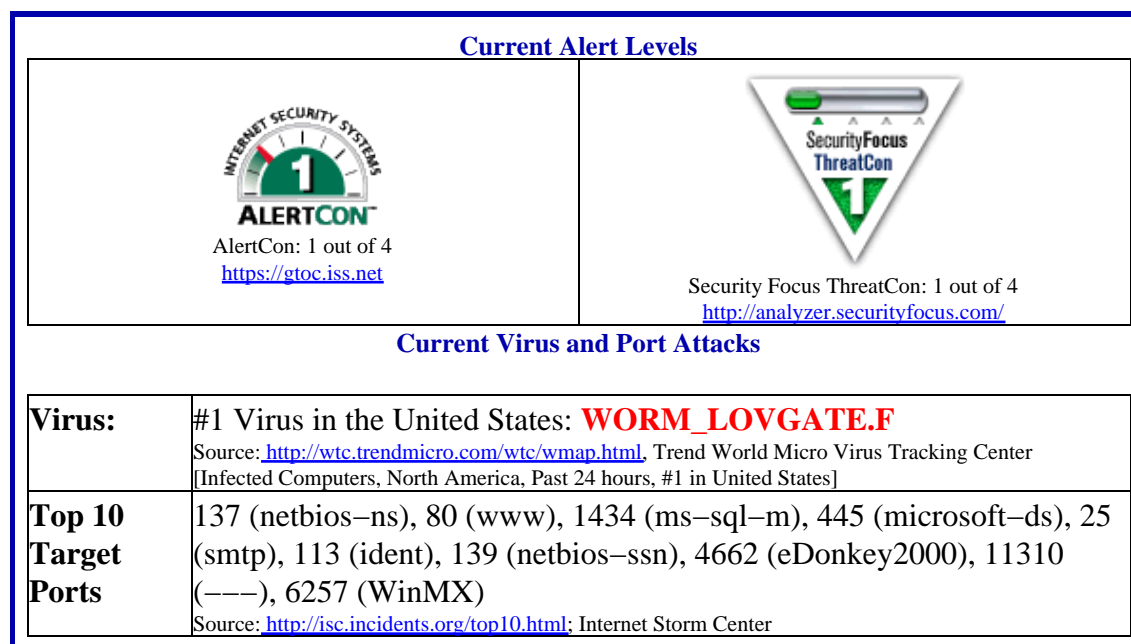
## **Information and Telecommunications Sector**



21. *April 30, Microsoft* — **Microsoft Security Bulletin MS03–016: Cumulative Patch for BizTalk Server.** There are two vulnerabilities in Microsoft's BizTalk Server. The first vulnerability affects Microsoft BizTalk Server 2002 only. **A buffer overrun exists in the HTTP receiver** and could result in an attacker being able to execute code of their choice on the BizTalk Server. The second vulnerability affects both Microsoft BizTalk Server 2000 and BizTalk Server 2002. **A SQL injection vulnerability exists in some of the pages used by DTA** that could allow an attacker to send a crafted URL query string to a legitimate DTA user. If that user were to then navigate to the URL sent by the attacker, he or she could execute a malicious embedded SQL statement in the query string. **Microsoft has assigned a risk rating of "Critical" to this vulnerability, and a patch is available at the Microsoft website:** <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03–016.asp>.  
Source: <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03–016.asp>
22. *April 30, IDG News Service* — **DHS asks for tech help.** Tom Ridge, secretary of the Department of Homeland Security (DHS), highlighted his department's need for technological innovations during a speech for members of the Northern Virginia Technology Council in Virginia, Tuesday. **Ridge also called for the technology industry to do more to protect the U.S. technology infrastructure**, noting that private companies control 85 percent of the nation's cyber resources. **"We think that the lessons learned from Y2K and 9/11 should be applied and not forgotten.** Ridge said he fears that some U.S. residents may be "lapsing into complacency" about the possibility of terrorist attacks. **"You need to be just as worried, maybe even more worried, about somebody hacking into your system as somebody pulling up with explosives,"** Ridge said. Ridge asked the crowd for "good ideas and cost-effective solutions" for domestic security that can be copied across the U.S.  
Source: <http://www.pcworld.com/news/article/0,aid,110514,00.asp>
23. *April 29, eWEEK* — **Vulnerability puts Oracle9i at risk.** A new vulnerability in Oracle Corp.'s database software puts not only the information in the database at risk, but in some cases, also can lead to a compromise of the operating system. The vulnerability is in the service that enables users to create links between two Oracle databases. In order to exploit the flaw, an attacker would need to send an overly long parameter with the connect string with a query to create a database link. This would trigger the stack buffer overflow, which would in turn overwrite the saved return address on the stack. This would give the attacker the ability to run any code he chose on the vulnerable server. **The vulnerability affects Oracle 9i Release 1 and 2; all releases of 8i; all releases of 8; and 7.3.x.** A patch is available at the Oracle website: <http://otn.oracle.com/deploy/security/pdf/2003alert54.pdf>.  
Source: <http://www.eweek.com/article2/0,3959,1047710,00.asp>
24. *April 29, Associated Press* — **U.K. arrests 'Fluffi Bunni' hacker.** Lynn Htun, the man thought to be the leader of a group of hackers known as "Fluffi Bunni," was arrested Tuesday by British authorities. **Fluffi Bunni captured the attention of the FBI just days after the September 11 terror attacks, when thousands of commercial Web sites were vandalized with a single break-in that included the message, "Fluffi Bunni Goes Jihad."** The FBI characterized the act in a November 2001 report as an anti-American cyberprotest against the war on terrorism.

Victims have included the Washington-based SANS Institute, Security Focus, and Attrition.org, a site run by experts who formerly tracked computer break-ins.  
Source: <http://www.siliconvalley.com/mld/siliconvalley/news/5745576.htm>

## Internet Alert Dashboard



[\[Return to top\]](#)

## General Sector

25. *April 30, Associated Press* — **Pakistan arrests suspect in Cole bombing.** A suspect in the suicide bombing of an American destroyer off the coast of Yemen was among six suspected al-Qaida men arrested in two simultaneous raids in southern Karachi, an Interior Ministry official said Wednesday. **Waleed Mohammed Bin Attash, who also is known as Khalid al-Attash, is wanted in connection with the suicide bombing of the USS Cole that killed 17 American sailors, the official said. The arrests were made Tuesday in two raids conducted by Pakistani law enforcement officers.** "This is a big catch. Al-Attash is wanted in the USS Cole bombing," said Brig. Javed Iqbal Cheema. "I think he is very important." He said the six al-Qaida suspects are still in Pakistan. The identities of the other men were not immediately known.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A59224-2003Apr 30.html>

26. *April 30, Associated Press* — **First Bali bombings suspect charged.** Indonesian prosecutors on Wednesday charged the first suspect in last year's Bali terror bombings that killed 202 people, mostly foreign tourists. **The suspect, known by the single name Amrozi, is one of 32 people detained on suspicion of involvement in the Oct. 12 attack. His arrest Nov. 5 was considered the first major break in the investigation. Antasari Ashar, a spokesman for the prosecution, said Amrozi had been charged with violating the country's new anti-terror laws. If convicted, he faces a maximum punishment of death. His trial is expected to begin**

in mid-May. Amrozi is alleged to be a member of Jemaah Islamiyah, the al-Qaida-linked regional terror group that has been blamed for the near-simultaneous bombings at two Bali nightclubs.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A58270-2003Apr 30.html>

27. *April 30, New York Times* — **Suicide bomber hits Tel Aviv. Shortly after 1 a.m., a security guard outside Mike's Place, which is steps from the American Embassy, confronted a fat man he apparently thought looked suspicious, witnesses said. It was the weekly "Jam Night," when musicians bring their guitars and saxophones for impromptu sessions, and the small bar was packed. The blast tore open the front of the bar and splattered blood on the trunk lid of a white sedan 100 feet away. There was no immediate claim of responsibility. The bar drew patrons from the embassy next door, as well as many American and British music and soccer fans. More than 30 people were wounded, officials said.**

Source: <http://www.nytimes.com/2003/04/30/international/middleeast/30MIDE.html>

28. *April 30, Washington Times* — **Iraqi lawyer who saved Pfc. Lynch granted U.S. asylum. Mohammed Odeh Al Rehaief, 33, along with his wife and 5-year-old daughter, were given asylum during a closed-door session on Monday in Arlington, allowing him to live and work in America and eventually apply for U.S. citizenship. Al Rehaief and his family arrived in this country April 10 after the Department of Homeland Security approved them for "humanitarian parole," which led to their asylum grant by the department's Bureau of Citizenship and Immigration Services.**

Source: <http://www.washingtontimes.com/national/20030430-11279215.htm>

[[Return to top](#)]

### **DHS/IAIP Products & Contact Information**

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web-site (<http://www.nipc.gov>), one can quickly access any of the following DHS/IAIP products:

[DHS/IAIP Warnings](#) – DHS/IAIP Assessments, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

[DHS/IAIP Publications](#) – DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

[DHS/IAIP Daily Reports Archive](#) – Access past DHS/IAIP Daily Open Source Infrastructure Reports

**[DHS/IAIP Daily Open Source Infrastructure Report Contact Information](#)**

Content and [nipcdailyadmin@mail.nipc.osis.gov](mailto:nipcdailyadmin@mail.nipc.osis.gov) or contact the DHS/IAIP Daily Report Team at  
Suggestions: 202-324-1129

Distribution Information Send mail to [nipcdailyadmin@mail.nipc.osis.gov](mailto:nipcdailyadmin@mail.nipc.osis.gov) for more information.

### **Contact DHS/IAIP**

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at [nipc.watch@fbi.gov](mailto:nipc.watch@fbi.gov) or call 202-323-3204.

### **DHS/IAIP Disclaimer**

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open-source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.